VTT Technical Research Centre of Finland

A survey on the use of PRA to support failure tolerance analyses

Karanta, Ilkka; Björkman, Kim

Published: 09/03/2020

Document Version
Publisher's final version

RESEARCH REPORT

VTT-R-00192-20

A survey on the use of PRA to support failure tolerance analysis

Authors: Ilkka Karanta, Kim Björkman

Confidentiality: Public

Report's title A survey on the use of PRA to support failure tolerance analysis	
Customer, contact person, address VYR	**Order reference** SAFIR 3/2019
Project name New developments and Applications of PRA	**Project number/Short name** 122529/NAPRA
Author(s) Ilkka Karanta, Kim Björkman	**Pages** 28/
Keywords failure tolerance analysis, YVL guide, probabilistic risk analysis	**Report identification code** VTT-R-00192-20

Summary

The purpose of STUK's YVL Guide B.1 is to assure that a nuclear power plant's systems, structures and components are designed and dimensioned in such a way that they are able to perform their function in all scenarios they are supposed to. A central requirement concerning this is failure tolerance, which informally means that a failure cannot spread across the system: the system will fill safety requirements even though some parts of it have failed. Failure tolerance analysis (FTA) is a framework to organize individual analyses that demonstrate this for some given part of the system to a systematic and comprehensive whole.

To clarify the concept of FTA, and the potential role of probabilistic risk assessments (PRA) as a part of it, a survey was conducted among the Finnish nuclear power companies and STUK. This report describes the result of that survey.

There are several requirements in YVL B.1 whose fulfilment can be demonstrated by FTA. In their answer, STUK gives a list of examples, and notes that FTA can be used in the treatment of requirements in some other YVL guides, too.

The experience on FTA varies from company to company. Fennovoima has not conducted FTA yet but will do so as a part of construction license application. Fortum has conducted FTA for plant modifications, and to the scope of the modifications only. TVO has conducted a top-level FTA for OL1 and OL2, failure modes and effects analysis for PRA, and certain other analyses for some systems; for OL3, several systems have been analysed in the FTA framework.

From STUK's reply it is clear that PRA is not a promising approach to support FTA, because in PRA it is generally assumed that systems can fulfil their function if no part of it has failed, whereas the purpose of FTA is to demonstrate this.

The repliers also present some ideas and views concerning the scope and properties of a method for FTA. These will help future development work in FTA.

Confidentiality	Public

Espoo 9.3.2020

Written by	**Reviewed by**	**Accepted by**
Ilkka Karanta senior scientist	Tero Tyrväinen research scientist	Nadezhda Gotcheva research team leader

VTT's contact address

VTT Technical Research Centre of Finland Ltd, P.O. Box 1000, FI-02044 VTT, FINLAND

Distribution (customer and VTT)

SAFIR2022 RG2 members, VTT archive

Preface

This report describes the results of a survey on failure tolerance analysis carried out in 2019. The report is a deliverable of the New Developments and Applications of PRA (NAPRA) project which is a part of the Finnish SAFIR2022 research programme. The authors wish to thank the experts of the responding organizations who participated in answering the questionnaire.

Espoo 9.3.2020

Authors

Contents

1. Introduction

This report describes the results of a query to the Finnish nuclear power companies and the Radiation and Nuclear Safety Authority in Finland (STUK) concerning failure tolerance analyses (FTA). FTA is a new concept that gained significance in the Finnish nuclear safety context in the YVL guide B.1 in 2013 [7]. Shortly put, the aim of FTA is to show that all systems performing safety functions and their auxiliary systems satisfy the failure criteria related to defence-in-depth requirements for a nuclear power plant. The requirement to conduct FTA is new, meaning that few examples of such analyses exist and there are several open issues on how to perform them.

In the summer of 2019, STUK released a substantially revised version of the YVL B.1 guidance document [8], and there the requirements of FTA were clarified.

To clarify issues related to FTA and its role in the safety design of nuclear facilities, a survey was carried out among the Finnish nuclear safety stakeholders: the nuclear power plant (NPP) companies Fennovoima, Fortum and Teollisuuden Voima (TVO), and STUK. The survey consisted of a questionnaire (see Appendix) that was sent to the stakeholders. All stakeholders replied to the query. This report describes the replies received.

The report is structured as follows. In section 2, an attempt is made to clarify the definition of FTA and its context. In section 3, examples of YVL B.1 requirements whose fulfilment can be demonstrated by FTA are listed for ease of reference. In section 4, the experiences of the Finnish nuclear power companies, as reported in the replies, are presented. Section 5 tries to clarify the role of PRA in satisfying YVL B.1 requirements. Section 6 considers the question to what extent PRA can be used in FTA. Section 7 reports the repliers' view on what kind of reliability analysis method development would best serve the needs of FTA. Section 8 concludes this report. In the Appendix, the original survey questionnaire is provided.

2. Failure tolerance analysis

Representatives of STUK [2] define failure tolerance informally in the following way:

> Failure tolerance analysis is a collection of analyses aimed at demonstrating that NPP design and construction fulfils failure tolerance requirements set forth in YVL guides.

They emphasize that FTA is not a single analysis, but rather a framework to organize failure analyses into logical parts. In their reply to the query, STUK gives the following examples of failure analyses involved: failure modes and effects analysis (FMEA), common cause failure analysis, redundancy and diversity analyses, interface analysis, hazard analyses, analyses of spurious instrumentation and control (I&C) actuations. The constituent analyses are mainly familiar, but some new approaches are needed for common cause failure (CCF) and diversity analysis, and for I&C active failure analysis [2].

In their reply to the query, STUK clarifies the nature of FTA:

> Primary target of FTA is to demonstrate the fulfilment of deterministic requirements. Individual analyses are more detailed and they contain more specific information than PRA.

The historical background for the emergence of FTA is that there were several issues regarding failure analyses required in YVL guides [2]. Certain issues were tackled in separate disciplines with disconnected analyses, some analyses and work overlapped yet there were gaps that the analyses did not cover, boundaries between and acceptance criteria of analyses were unclear, and there were difficulties in performing, reviewing and understanding the plant as a whole. These difficulties pointed to the need for a holistic approach to complement analyses focusing on single systems or viewpoints. STUK conducted an interdisciplinary project for I&C failure analysis in 2012-2013, and a Master's thesis [1] was written where individual analyses of Olkiluoto 3 were organized into a whole, grouping them according to the entities and safety principles considered.

The regulatory importance of FTA is embodied in the YVL Guide B.1 [8], section 3.6, where paragraph 351 states

> The fulfilment of the failure criteria of systems implementing safety functions and their support systems as well as common cause failures shall be assessed by means of failure tolerance analysis when designing the systems or their modifications. If necessary, analyses shall be performed in more detail in different stages of design.

It is useful to contrast failure tolerance, as STUK has specified it, to fault (or failure) tolerance as it is specified in the context of computers and data networks [5], from system design and verification point of view. The definition of failure is similar to that used in PRA, and it is recognized that "faults and errors can spread through the system". Further, a general design principle in that field is to incorporate barriers (called containment zones) into computing systems that "reduce the chance that a fault or error in one zone will propagate to another". However, [5] states that "all of fault tolerance is an exercise in exploiting and managing redundancy"; this implies that the defence-in-depth safety principles framework widely adapted in the nuclear safety field is broader than the one used in the computing systems community because it covers also separation, diversity and other safety principles of the defence-in-depth concept.

Concerning the scope of FTA, STUK states in the reply to the query that

FTA should consider all safety functions, and all systems and their subsystems implementing safety functions. FTA utilizes system-FMEA, and each component that may affect the system shall be included in system-FMEA ([8] 351, 352),

3. Failure tolerance analysis in YVL B.1 requirements

In their reply to the query, STUK lists some examples of YVL B.1 requirements that can be demonstrated by FTA. They are 351, 352, 353, 421c, 429, 431, 432, 433, 435, 437, 5240, 5241. STUK notes that there are also other requirements that can be demonstrated by FTA, including requirements in other YVL guides such as D.3: 414-417; E.11: 515, 521, 620. Further, STUK emphasizes that these lists should not be used as such for example in the interpretation of YVL guides. For convenience of reference, the above-mentioned YVL B.1 requirements are listed here.

351. The fulfilment of the failure criteria of systems implementing safety functions and their support systems as well as common cause failures shall be assessed by means of failure tolerance analysis when designing the systems or their modifications. If necessary, analyses shall be performed in more detail in different stages of design. [2019-06-15]

352. A failure tolerance analysis shall assess one functional complex at a time, with due regard both to the system that performs a safety function and its auxiliary systems. The analysis shall address each component that, in the event of a failure, may affect the successful execution of the safety function performed by the system following a specific initiating event. The analysis shall address all modes of failure for all the components affecting the system performing the safety function. Depending on the applicable failure criterion, the analysis shall focus on one or multiple failures at a time and examine their impact in terms of the operation of the system. [2019-06-15]

353. A common cause failure analysis shall be drawn up for anticipated operational occurrences and class 1 postulated accidents. For the common cause failure analysis, the implementation of the safety functions shall be presented for each initiating event in a manner that indicates the use of the systems implementing the principles of diversity and redundancy. The common cause failure analysis shall address one safety function, or part of it, at a time with due regard to the systems implementing the function and the related auxiliary systems. The analysis shall address the common cause failures of all components whose common cause failures or spurious actuation may affect the performance of the safety function. The common cause failure analysis shall consider the initiating event, their consequential effects as well as common cause failures between components sharing a similar property, i.e. components that are similar or contain a significant number of similar parts. [2019-06-15]

421c. A common cause failure of any individual component type (for example, a similar check valve, same type and manufacturer) shall not prevent the nuclear power plant from being brought to a controlled state or a safe state. [2019-06-15]

429. The systems required for implementing different levels of defence according to the defence-in-depth principle shall be functionally isolated from one another, in such a way that a failure on one level shall not prevent the implementation of necessary functions at other levels of defence. [2019-06-15]

431. The systems intended for reaching and maintaining a controlled state in severe reactor accidents (level 4 of the defence in depth concept) shall be functionally and physically separated from the systems intended for normal operation and anticipated operational occurrences and for controlling postulated accidents and design extension conditions (levels 1, 2, 3a and 3b). The defence-in-depth level 4 systems intended for controlling severe reactor accidents may, for sound reasons, also be used for preventing severe core damage in design extension conditions provided that this will not undermine the ability of the systems to perform their primary function in case the conditions evolve into a severe reactor accident. [2019-06-15]

432. No single anticipated failure or spurious action of an active component taking place during normal plant operation shall lead to a situation requiring intervention by systems designed to manage postulated accidents. [2013-11-15]

433. Provisions shall be made for failures by ensuring that systems performing a safety function consist of two or more redundant systems or system parts in parallel, so that the safety function can be performed even if any of them is rendered inoperable. [2013-11-15]

435. The failure of a subsystem in a system executing safety functions shall not cause the failure of another redundant subsystem of the same system or the failure of several subsystems participating in the same safety function. [2019-06-15]

437. The safety divisions hosting redundant parts of safety systems shall be located in different buildings or housed in dedicated compartments to separate them from the other safety divisions in the same building in order to prevent faults from spreading from one redundant system part to another as a result of internal events (e.g. fire, flood or dynamic effects) or external events. [2019-06-15]

5240. The consequences of I&C failures shall be limited in accordance with the following requirements in so far as they are not already limited by other requirements:

1. A failure of class EYT I&C as an initiating event shall not lead to consequences that are worse than an anticipated operational occurrence.

2. A failure of class EYT I&C during anticipated operational occurrences and accidents shall not essentially degrade the plant state (the acceptance criterion of the event remains within the same event class).

3. A failure of safety class 3 I&C as an initiating event shall not lead to consequences that are worse than a class 1 postulated accident.

4. A failure of safety class 3 I&C in connection with an anticipated operational occurrence shall not lead to consequences that are worse than a class 1 postulated accident.

5. A failure of safety class 3 operational and limitation I&C during accidents shall not essentially degrade the plant state.

6. A failure of safety class 3 back-up protection system or safety class 3 severe reactor accident I&C shall not essentially degrade the plant state In postulated accidents. [2019-06-15]

> 5241. The effects of the failures and errors of the controls and functions performed by the I&C systems shall be analysed as functional entities. Functional entities may consist of system-internal structures, and they may cross the interfaces between systems. The functional entities selected for analysis shall be justified. The analysis shall account for all possible failure modes of the I&C systems. The analysis shall demonstrate that the I&C systems meet the requirements concerning failures. [2019-06-15]

4. Experiences with failure tolerance analysis

Fennovoima tells about their status with regard to FTA, and their plans related to it as follows:

> We have not yet conducted a failure tolerance analysis for the NPP but will it will be done as a part of the construction license application. All systems performing safety functions (front-end-systems) and all supporting systems will be analysed.
>
> We will address the requirements YVL B.1 351, 352. Additionally, requirements 425, 428, 429, 431, 433, 435, 442, 446, 448, 449, 455, 456, 5105 are addressed to some extent.
>
> The specification for failure tolerance analyses is still under development so the methods are not final. The method intended to be used is a combination of qualitative reliability analysis (in the same manner as FMEA) and then constructing a logical model based on this information. Analysis cases will be developed based on the model constructed and MCSs [*minimal cut sets*] generated. The MCSs will be analysed and based on that it will be assessed whether the requirements are met.

Fortum has conducted FTA:

> We conduct failure tolerance analysis in case on plant modifications and to the scope of modifications only. The analysis have been described in the NPP instructions for conceptual design plan and pre-inspection plan for system modifications.
>
> We have conducted following analysis:
>
> - common-cause failure analysis of selected transmitter rooms, the transmitters were in the scope of I&C renewal ELSA and project SETU2.
> - analysis on the effects of the actuation mode change into failure tolerance of safety functions actuating emergency feedwater actuation, project SETU2
> - common-cause failure analysis of the scope of automation renewal. Scope of renewal was part SC2, SC3 and NS functions.
> - failure tolerance analysis of components that had insufficient safety class separation
>
> The analysis were conducted on component, safety function, automation system and automation platform levels, depending on the analyzed scope. In the analysis we addressed YVL B.1 requirements 351-354, 425-430, 5236-5241, depending on the analyzed scope. The methods used have mainly been normal engineering work and common tools like MS Word and Excel. Some expertise has been

purchased from external sources for thorough automation diagram functional level failure modes analysis FMEA.

We did not find any special issues during the analysis. Some development to methods and tools would be beneficial.

We will conduct FTAs in the future at least for some safety functions and their components. No problems foreseen.

TVO has also conducted FTA to some degree:

OL1/OL2

An FMEA has been performed for systems included in the PRA.

A top-level FTA concerning safety functions (control of criticality, pressure control of RCPB [*reactor coolant pressure boundary*], reactor cooling, heat transfer to UHS [*ultimate heat sink*], containment function) is presented as a topical report to the FSAR [*final safety analysis report*].

In addition, we have performed specific analyses of failure tolerance to certain components and systems (e.g. time relays, electrical breakers, electrical busbars).

Main issues were how to interpret the YVL B.1 requirements and what is the expected form of presentation.

OL3

Following analyses have been performed:

Automation FMEA

Process and electrical systems FMEA

Protection system analysis of the compliance with the N+2 criteria

I&C architecture CCF analysis

I&C architecture defence in depth and diversity analysis

I&C failure analysis

Diversification and CCF analysis

5. Use of PRA in YVL B.1

STUK states the following:

The purpose of YVL B.1 is to assure that the SSCs [*systems, structures and components*] in an NPP are correctly designed and dimensioned, so that structures, systems and components have enough capacity and functionality to perform their function for scenarios they are intended to operate in.

PRA does not deal with physical design errors. Instead, PRA assumes that systems are correctly dimensioned so that they fulfil their tasks if SSCs are functional. Thus, the role of PRA in revealing design errors is quite limited.

> In short, the role of PRA is not related to functionality, but to the reliability of maintaining the functionality as designed.
>
> Based on this, PRA can be applied in the demonstration of the following YVL B.1 (2019) requirements: 350, 413, 421d, 423, 423a, 424, 428, 447, 450a, 455a, 5418, 5453

Fennovoima considers that the following YVL B.1 requirements are such that PRA can be used in their satisfaction. They also state that other requirements in YVL B.1 are not such that PRA could be well utilized, although they imply that this assessment is based on a quick glance through the requirements.

> YVL B.1 350, 421, 424, 428, 439, 450, 453, 455, 458, 5104, 5240, 5241, 5302, 5310, 5418, 5426.
>
> 350, 421, 424, 428 particularly. These are direct requirements related to the quantification of risk where PRA is practically the best tool available.

Fortum sees PRA's role in assessing the satisfying of YVL B.1 requirements as quite limited:

> The listed B.1 requirements are deterministic by nature. Therefore PRA may only be used to provide input data (in case FTA has similar needs) or to justify configurations that may not fulfill all deterministic requirements.
>
> The listed requirements should be primarily analysed without PRA, to maintain the ability to provide insights independently. Assumptions made in PRA should not guide the deterministic analyses too much. There are separate YVL requirements that discuss the use of PRA.

TVO sees PRA's role as follows:

> Similar methods may be used to conduct an FTA as are used to perform a PRA.
>
> The analysis of dependencies between different types of failures and consequences on plant level in various situations is such a complex issue that modelling techniques like PRA are usually needed.

TVO sees the limitations of PRA in this context as follows:

> Not all issues are treated in enough detail in a PRA that it is usable for an FTA, e.g. automation architecture.
>
> PRA is a best-estimate analysis whereas deterministic analyses are often more conservative.

6. The relationship between PRA and FTA

Concerning the role of PRA in FTA, STUK states that

> PRA shall be used in definition of DEC [*design extension condition*] B.
>
> Otherwise PRA is not applicable to failure analyses. PRA is based on failure analyses and the PRA model contains only those features that have already been identified in failure analyses.

DEC-B is design extension condition with core melt [3].

STUK justifies their view that PRA is not useful in FTA as follows:

> PRA-models are simpler than failure analyses. For example, if a failure analysis demonstrates that a failure does not spread from one system to another, it is not necessary to model the spreading in PRA. FTA identifies issues that have to be included in the PRA model. The same applies to design rules in early design phase. If, for example, a design rule is such that a component shall be powered at least from two trains, PRA model is based on this rule.
>
> For CCF analyses, in redundant/diverse systems that participate in a safety function, it is necessary to identify similar components performing similar functions. This identification process is central part of a CCF analysis. PRA model is then based on the identification performed in CCF analysis. In order to review the PRA model, it is necessary to return to the underlying CCF identification process. Indeed, PRA model can produce different kinds of cut sets and failure combinations, but they can not be taken for granted. To review the correctness of cut sets and failure combinations, it is necessary to review the failure analyses and their implementation in the PRA model. Our opinion is that PRA produces only little, if any, additional insights into FTA.
>
> For example, failure tolerance analyses separated of I&C entities (B.1 5240, 5241): Such FTA is performed, e.g., by treating a separated I&C entity as a black box and identifying the worst possible combination of its output signals, with additional DBC2-DBC3 initiating event and without it. The resulting plant behaviour is compared to deterministic acceptance criteria.

Further, STUK elaborates on not using PRA in FTA as follows:

> STUK will not review FTA which is based on PRA.
>
> Failure tolerance analyses are the collection of diverse analyses, which together demonstrate that the NPP in question tolerates failures as required in YVL Guides.
>
> PRA deals with core damage. The acceptance criteria of FTA are different, and only rarely are compatible with core damage. Most of the acceptance criteria are deterministic and explicitly stated. E.g. YVL B.1 5240 and 5240 describe a set of acceptance criteria, whose fulfillment can mostly be demonstrated by identifying enveloping deterministic design-basis safety analyses.
>
> Normal PRA model is way too simplistic to be used for FTA. Thus, FTA should be based on more complex PRA model, and such a model should be reviewed for use of failure tolerance modelling. However, such a review is possible only against analysis of failure propagation and tolerance, i.e. failure tolerance analyses.

On the other hand, STUK sees that FTA is a very useful, or even a necessary prerequisite to PRA:

> FTA can benefit PRA greatly. In fact, it is nearly impossible to perform PRA without FTA.

Some justification to this claim is as follows [6]:

> Contents of the logical model of a PRA (e.g. what to model and what not to) is derivable from failure analyses. Thus, the PRA model readily includes the results of failure analyses. FTA is a failure analysis, and with it one may for example

> verify that things have been excluded from PRA correctly because according to analyses a fault does not propagate.
>
> [..]
>
> If a failure tolerance analysis demonstrates that a failure e.g. does not propagate from a lower safety class to an upper one, such propagation will naturally not be modelled in PRA.

Fennovoima has not used PRA in FTA, because they have not conducted FTA yet:

> Our project is at such a stage that FTA specification is still under development which is why the actual analyses have not yet been performed.

Nevertheless, Fennovoima considers that PRA is useful in FTA. They appraise its role as follows:

> PRA can help in the development of the qualitative reliability analysis and in constructing the FTA model.
>
> [*On the most useful aspects and uses of PRA in FTA*] FMEA, constructing the FTA model. The MCSs list can also be reviewed to check if some inconsistencies with the FTA requirements can be spotted right away.
>
> [*On whether FTA can benefit PRA*] I guess it can. Remains to be seen, when the actual FTA has been developed.
>
> [*On which parts of the plant PRA model could be utilized*] Whole model can probably act as a basis for constructing the FTA model.
>
> [*On what parts of the PRA model would have to be modified or constructed for FTA, and what FTA analysis tasks are better left to other methods than PRA*] Some parts have to be probably modified if simplifications have been done or conservatisms have been integrated into the model because of simplicity. Human errors are probably handled better through the HFE program, but FTA is a good tool for checking the fulfillment of the redundancy and diversity requirements.

Fortum sees that PRA can be used in FTA, but only in a very limited way:

> [*Is PRA useful in FTA*] In a sense, yes.
>
> PRA may be used to justify certain configurations when FTA shows that all deterministic requirements are not fulfilled - if the risk significance is low enough.
>
> The use of probabilities and ability to estimate risk significance make it possible to justify relaxation of overly strict deterministic requirements. The basic assumptions may be highly different between FTA and PRA and therefore they may provide different insights and supplement each other well. E.g. FTA does not consider all failure combinations, but PRA does.
>
> [*What supporting analyses would be needed to support PRA for FTA*] FMEA.
>
> FTA and PRA may use similar input data, such as FMEA.

Fortum has not used PRA in FTA, and explains the main reason as follows:

> It is beneficial to keep PRA independent, to gain insights from different viewpoints.

Concerning the role that PRA could play in the analyses, Fortum refers to its previous answers (see above). They further specify:

> The whole PRA model is used to gain risk insights.

Fortum does not anticipate that PRA models (fault trees, event trees etc.) would be modified or constructed for FTA. They justify this as follows:

> PRA models do not generally provide enough detail to conduct FTA based on the fault trees.

TVO considers that PRA is useful in FTA:

> FMEA and CCF analyses have been performed for the PRA. These may be used as a part of a FTA.
>
> PRA highlights the dependencies between the main systems through their support systems. Consequences of internal and external hazards are evaluated in the PRA.

TVO also states that FTA can benefit PRA:

> The PRA may be built from a perfect FTA and vice versa. However, we have not used FTA or its result in the PRA.

TVO has used elements of PRA in FTA:

> FMEA is the backbone of our FTA together with information from the PRA. FMEA's for OL1/OL2 have been use for PRA purposes. We do not have an explicit FTA for OL1/OL2.

7. FTA development needs and ideas

STUK states that

> FTA deals with the entire NPP, unlike system-specific analyses. The global AIM of FTA is to demonstrate that the design and implementation of the safety functions of a NPP fulfil criteria concerning failure tolerance, diversity, independence and separation. Thus, for example, fire and flood analyses are part of FTA, and their aim is to demonstrate that necessary safety functions can be performed even when fire or flood destroys one safety compartment so that it behaves in worst possible way. For example, for I&C it is assumed that when it is destroyed by fire, it sends out worst possible output combination, and it shall be demonstrated that the plant can be managed with remaining I&C systems according to acceptance criteria as specified in YVL B.1 5240 and 5241.
>
> Detailed reliability models and analyses can be utilized in creating simpler PRA-models.

This may be interpreted as a statement of the view that reliability analysis approaches are not a promising, or even a suitable, approach to support FTA.

STUK also provided, as an appendix to their reply, an example demonstration of failure tolerance. The demonstration is in the form of a Microsoft Excel workbook consisting of a single

worksheet. It is short and generic, consists of analysis steps, and describes what systems would be analysed and in what ways, what purpose each analysis phase serves, and what open questions remain after an analysis phase (which lead to the next analysis phase). The system analysed is a generic nuclear power plant, with a focus on safety functions and I&C. The example analysis consists of 8 phases, and for each phase, a short description is provided of the analysis conducted, what the analysis demonstrates, and what questions remain concerning the analysis subject. STUK clarifies the contents and purpose of the example as follows:

> The demonstration is performed in steps, where one phase lays the foundation for the next phases. Each analysis has a well-defined scope, and together all analyses demonstrate that failure tolerance is fulfilled. NOTE that this is just an unofficial example and it cannot be used in justification of adequate analysis set.

Fennovoima has the following views concerning an approach to be developed for FTA:

> [*Which YVL B.1 requirements should the approach address*] It should address the [*YVL B.1*] requirements [*listed in Fennovoima's answers to questions 1 and 2 of the questionnaire. These are as follows: 351, 352. Additionally, requirements 425, 428, 429, 431, 433, 435, 442, 446, 448, 449, 455, 456, 5105 to some extent. Considering PRA specifically, requirements 350, 421, 424, 428, 439, 450, 453, 455, 458, 5104, 5240, 5241, 5302, 5310, 5418, 5426, and particularly 350, 421, 424, 428*]
>
> [*What systems should be analysable by the approach*] Safety automation and other automation in the extent if it can cause unavailability of safety systems through spurious actuations and signals.
>
> [*What kinds of results should the approach produce*] It should produce some kind of a suitable approach to identify the consequences of spurious signals. Additionally it should produce suggestions to modelling of the reliability of digital I&C as well (identification of CCFs).
>
> [*In what ways should the approach support PRA*] It should help in the development of the risk model construction. Parameters can be varied in later phases based on the information available.
>
> [*In what way(s) should the approach support failure tolerance analyses*] In the same manner as in [the previous paragraph], in constructing the logical model.

Fortum states the following concerning a prospective approach to support FTA and PRA:

> [*In what ways should the approach support PRA*] The approach should provide a model that is compatible with the existing plant PRA model (e.g. fault tree), including failure probabilities.
>
> [*In what way(s) should the approach support failure tolerance analyses*] The different failure modes and their occurrence could be directly used as input for FTA, where the failure consequences to the functional (safety functions) and plant level (plant response) can then be analyzed. Additionally, information on simultaneous faults of normal operating system could be used as an input for FTA.

Fortum does not have at the moment a case problem that could serve as a case for analysis in the development of the approach.

8. Conclusions

STUK's reply to the survey clarifies the scope and purpose of FTA, and the methods applicable in the endeavour. These are based on the purpose of YVL B.1, which is to "assure that the SSCs in an NPP are correctly designed and dimensioned" so that they can perform their intended function.

STUK states that FTA should not be based on PRA. However, STUK states that PRA deals with core damage, which apparently refers to the plant PRA model that NPP companies have to have for licensing; this still seems to leave open the possibility that PRA could be used in some minor role as a supporting analysis, perhaps with PRA models specially developed for some narrow purpose, or with PRA as an auxiliary analysis in special situations (e.g. in justifying certain configurations when FTA shows that all deterministic requirements are not fulfilled, by demonstrating that their risk significance is sufficiently low, as Fortum suggests). Nevertheless, PRA certainly does not offer a promising way to conduct FTA analyses. If a company identifies a natural role for PRA in supporting or complementing FTA, it seems advisable that they consult STUK before application attempts.

The experience of the NPP companies in conducting FTA to satisfy YVL B.1 requirements varies. Fennovoima has not conducted FTA yet, but will for the construction license. Fortum has conducted FTA for plant modifications, not for the full plant. TVO has conducted a top-level FTA concerning safety functions to OL1/2, and several system/component-specific analyses for OL1/2/3.

Concerning the development of an approach to the FTA of digital I&C, it can be concluded that an approach based reliability analysis proposed in the questionnaire is not fruitful. Instead, FTA calls for deterministic analyses. The short example FTA, provided by STUK as an appendix to its reply, helps development of such an approach by illuminating how an FTA can be structured, the issues involved in different phases of the analyses etc. Fennovoima sees safety automation, to the extent that it can cause unavailability of safety systems through spurious actuations and signals, as a fruitful scope for such an approach. Especially, the approach should involve constructing a logical model of the targeted system; this would also help in the development of the risk model.

References

[1] Pia Humalajoki. Ydinvoimalaitoksen vika-analyysit (failure analyses of nuclear power plant). Master of Science Thesis, March 2016, 82 pages (in Finnish).

[2] Pia Humalajoki, Ilkka Niemelä (STUK). NPP failure tolerance analyses. Presentation at the Nordic PSA Castle Meeting 2015, 8-10 September, 2015, Hotel Haikko Manor, Porvoo. 15 slides.

[3] International Atomic Energy Agency. Safety of nuclear power plants: design. Specific Safety Requirements No. SSR-2/1 (Rev. 1), IAEA 2016, 99 pages.

[4] International Atomic Energy Agency. Considerations on the application of the IAEA safety requirements for the design of nuclear power plants. IAEA-TECDOC-1791, 2016, 88 pages.

[5] Israel Koren, Mani Krishna. Fault-tolerant systems. Morgan Kaufmann Publishers, 2007.

[6] Ilkka Niemelä (STUK). Notes accompanying STUK's reply to the survey, 2019.

[7] Radiation and Nuclear Safety Authority STUK. Safety design of a nuclear power plant. Guide YVL B.1/15 November 2013. 46 pages.

[8] Radiation and Nuclear Safety Authority STUK. Safety design of a nuclear power plant. Guide YVL B.1/15 June 2019. 73 pages.

Appendix: the questionnaire sent to stakeholders

NAPRA — todennäköisyyspohjaisten riskianalyysien käyttöä vikasietoisuusanalyyseissä koskeva kysely

Tämän kyselyn tarkoitus on koota tietoa siitä, miten todennäköisyyspohjaista riskianalyysiä (probabilistic risk analysis, PRA) voidaan käyttää vikasietoisuusanalyyseissä (failure tolerance analysis, FTA). Kysely tehdään osana SAFIR2022-tutkimusohjelman rahoittaman NAPRA-projektin työpaketin 4 (Digital I&C reliability and risk analysis) osatehtävää 4.2 (Use of PRA to support failure tolerance analysis).

YVL-ohjeen B.1 (STUK 2013) mukaan FTA:n tarkoitus on osoittaa että ydinvoimalan kaikki turvallisuustoimintoja suorittavat järjestelmät ja niiden apujärjestelmät toteuttavat syvyyspuolustusvaatimuksiin liittyvät vikaantumiskriteerit. NAPRA-projektissa tehtävän FTA-tutkimuksen yksi motiivi on, että tämä vaatimus on suhteellisen uusi, sen toteuttavista analyyseistä on vain vähän esimerkkejä, ja FTA:n toteuttamisessa on useita avoimia kysymyksiä. Toinen motiivi on, että PRA:n ja FTA:n välillä on merkittäviä yhtymäkohtia, koska PRA on kattaa koko laitoksen ja PRA-malli sisältää myös yhteydet komponenttien, rakenteiden ja osajärjestelmien vikaantumisen sekä laitosyksikkötason toimintojen epäonnistumisen välillä.

Kyselyn sivuilta 2-4 löytyy kuvaus vikasietoisuusanalyyseistä YVL-ohjeen tarkoittamassa mielessä. Kuvaus on tarkoitettu taustoittamaan kyselyä ja helpottamaan kyselyyn vastaamista, mutta sen lukeminen ei ole välttämätöntä kyselyyn vastaamiseksi.

Olkaa hyvä ja vastatkaa suoraan vastauslaatikoihin. Pyydämme lähettämään vastauksen sähköpostin liitteenä osoitteeseen ilkka.karanta@vtt.fi

Tulokset tullaan julkaisemaan tutkimusraportissa, joka on NAPRA-projektin osatehtävän T4.2 kuluvan vuoden deliverable. Lisäksi on mahdollista, että joitakin kyselyssä saatuja tuloksia julkaistaan konferenssipaperissa tai tieteellisessä lehtiartikkelissa; mikäli ette halua että organisaationne vastauksia lainataan tällaisissa kansainvälisissä yhteyksissä, pyydämme ilmoittamaan asiasta kyselyn kohdassa 6 (yleiset kommentit).

Kiitos osallistumisesta kyselyyn!

Ystävällisin terveisin,
Ilkka Karanta ja Kim Björkman

Failure tolerance analysis

The following summary of failure tolerance analysis is based on [1].

The Finnish regulatory guides have required failure tolerance analyses (FTA) for demonstrating the redundancy, diversity and separation of safety functions and systems of nuclear power plants since 2013 [1]. FTA covers plant level functions (including both the main system and the support systems) instead of individual systems.

The goal of FTA is to encompass the general design principles of nuclear power plants, i.e. redundancy, diversity, and separation. Different types of analyses are required for demonstrating the principle and every principle should be covered individually to demonstrate failure tolerance for the whole plant.

FTA is not a separate analysis approach, but rather a collection of well-established failure analysis methods. The FTA includes e.g. the following failure analyses; failure modes and effects analysis, common cause failure analyses, redundancy and diversity analyses, analyses of spurious I&C actuations and human error analyses. In Figure 1, different types of analyses for demonstrating different design principles are presented. It illustrates the need for different types of analyses instead of one analysis of failure tolerance.

Different failure analysis methods are summarized e.g. in [2].

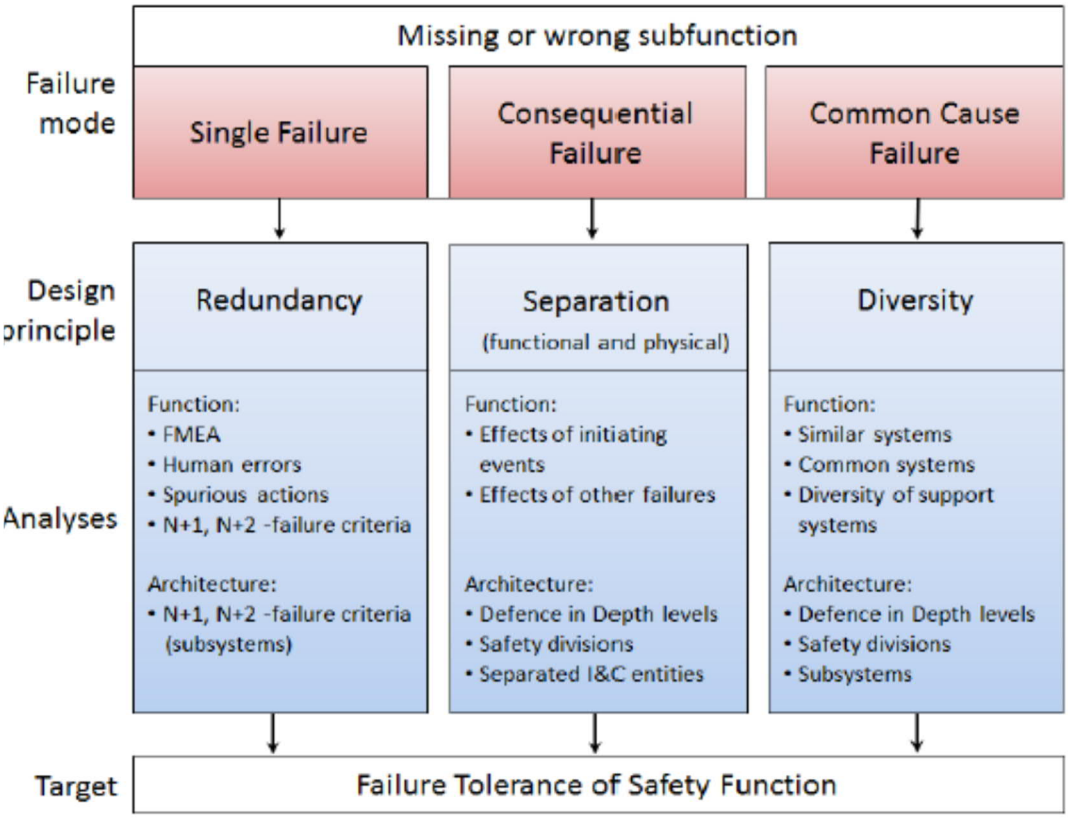

Figure 1. Individual parts of failure tolerance analysis and their targets [1].

YVL B.1 requirements for failure tolerance analysis

Failure tolerance analysis related requirements are given in [3]. The purpose of four FTA related requirements are described below (the requirements have been updated, changes are discussed below):

- The aim of failure tolerance analysis is stated in requirement 351. *"Failure tolerance analysis shall be carried out to demonstrate that*
    - *All systems performing safety functions and their auxiliary systems satisfy the failure criteria specified in section 4.3 of [YVL B.1]*
    - *Systems assigned to different levels of defence according to the defence in depth approach have been functionally isolated from one another in such a way that a failure in any one level does not affect the other levels; and*
    - *A common cause failure in any single component type (e.g. a similar check valve, same type and manufacturer) will not prevent the nuclear power plant from being brought to a controlled state and further to a safe state"*

- In requirement 352, the content to be covered by FTA is presented. *"A failure tolerance analysis shall assess one functional complex at a time, with due regard both to the system that performs a safety function and its auxiliary systems. The analysis shall address each component that, in the event of a failure, may affect the successful execution of the safety function performed by the system following a specific initiating event. The analysis shall address all modes of failure for all the components affecting the system performing the safety function. Depending on the applicable failure criterion, the analysis shall focus on one failure at a time and examine its impact in terms of the operation of the system."*

- Requirement 353 defines the scope for CCF analysis. It also covers a requirement to identify dependencies between initiating events and safety functions. *"A common cause failure analysis shall be drawn up for initiating events in design basis categories DBC 2 and DBC 3. For the common cause failure analysis, the implementation of the safety functions shall be presented for each initiating event in a manner that indicates the use of the systems implementing the principles of diversity and redundancy. The common cause failure analysis shall address one safety function, or part of it, at a time with due regard to the systems implementing the function and the related auxiliary systems. The analysis shall address the common cause failures of all components whose common cause failures or spurious actuation may affect the performance of the safety function. The common cause failure analysis shall consider the initiating event, interdependencies between initiating events as well as common cause failures between components sharing a similar property, i.e. components that are similar or contain a significant number of similar parts."*

- Requirement 354 requires that failure tolerance analyses shall consider human errors and demonstrate that single errors will not prevent the performance of the safety function concerned. *"Additionally, failure tolerance analyses shall consider human errors and demonstrate that single errors will not prevent the performance of the safety function concerned."*

The YVL B.1 requirements have been updated 15.6.2019 [4]. Therefore, also the above listed requirements have been updated. The changes has been justified in [5]. The new requirement 351, requires that failure tolerance analyses shall be performed. The previous demonstration requirement related to common cause failures has been changed to a design requirement in chapter 4. Requirement 353 has been clarified both concerning the terminology and the implementation of the diversity principle. Requirement 354 has been removed, since it was considered already to be included in failure analyses.

Relations between FTA, PRA and deterministic safety analysis

In Figure 2, the relationship between failure analyses, PRA and deterministic safety analyses is illustrated. The different approaches have their own different roles to assign the safety of

nuclear power plant. Deterministic methods demonstrate that the plant is able to accomplish the safety functions needed, even in case of selected failures (identified e.g., by failure analyses). PRA compiles the results of deterministic safety analyses and failure analyses to a risk model of the plant.

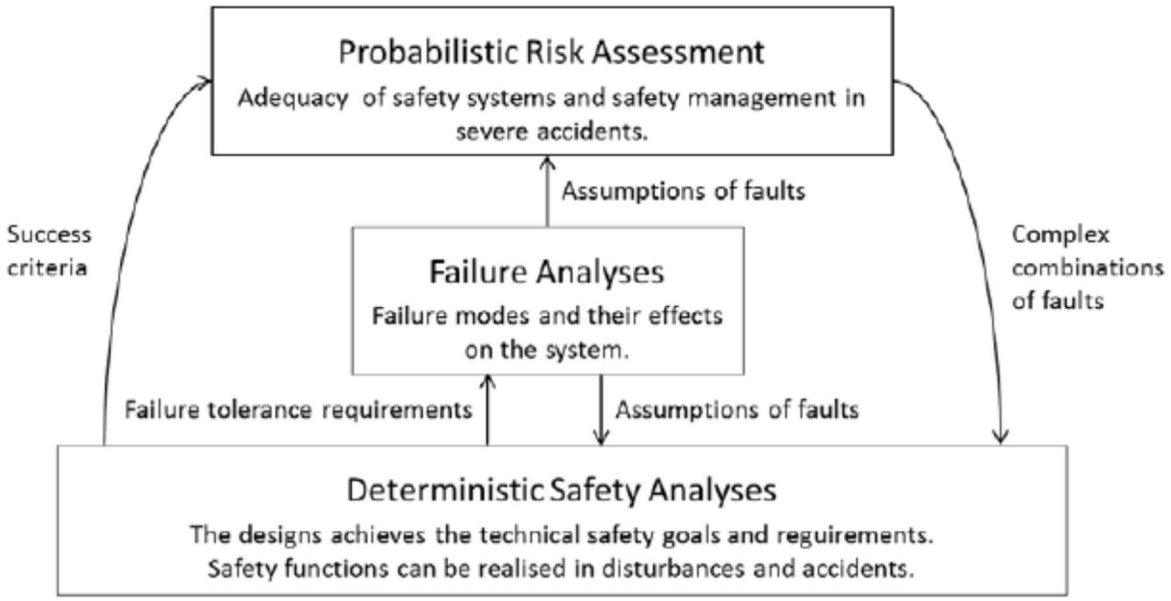

Figure 2. Relations between failure analyses, PRA and deterministic safety analyses [1].

The comparison of PRA, deterministic safety analyses and failure analyses results can affirm the coverage of the failure analyses set. When the analyses provide similar results, it will support the validity of the results. On the other hand, if the results differ, it raises the question on the validity or conclusion of the analyses.

Failure analyses, deterministic safety analyses and PRA together create a base for practical elimination concept in Finland. For further information see [6].

References

1. Humalajoki, P., Niemelä, I., Suikkanen, P., NPP Failure analyses in Finland, Probabilistic Safety Assessment and Management PSAM 14, 2018, Los Angeles.

2. Humalajoki, P., Ydinvoimalaitoksen vika-analyysit, Master's Thesis, Tampere University of Technology, pp. 82, 2016.

3. Radiation and Nuclear Safety Authority (STUK), Safety design of a nuclear power plant, Regulatory Guide YVL B.1, 15.11.2013, Helsinki. https://www.stuklex.fi/en/ohje/YVLB-1

4. Radiation and Nuclear Safety Authority (STUK), Ydinvoimalaitoksen turvallisuussuunnittelu, Regulatory Guide YVL B.1, 15.6.2019, Helsinki. https://www.stuklex.fi/en/ohje/YVLB-1

5. Radiation and Nuclear Safety Authority (STUK), Ohje YVL B.1, Ydinvoimalaitosten turvallisuussuunnittelu - Perustelumuistio, 102/0002/2016, 15.6.2019, Helsinki. https://www.stuklex.fi/fi/YVLB.1-perust.pdf

6. Niemelä, I., Lahtinen, N., Marjamäki, M., Practical Elimination - Experiences for Units in Use, in Construction and in Design, Probabilistic Safety Assessment and Management PSAM 14, 2018, Los Angeles, CA.

1) Have you conducted a failure tolerance analysis (FTA)?
    a. if you have, what subsystems/components/structures and safety functions were included in the analysis?
    If you addressed YVL B.1 requirements, which requirements were they?
    What methods did you use?
    What were the main issues and open problems encountered during the analysis and its reporting?
    b. If you have not, are there any structures, systems or components (SSCs) for which you would expect to conduct an FTA in the next few years?
    What kinds of problems would you expect to face upfront?

2) Use of PRA in YVL B.1
   a. In your view, what requirements in YVL B.1 are such that PRA can be used in assessing whether they are satisfied?
      Which of these requirements are such that PRA is particularly suited in their assessment?
      Why (please note that the role of supporting analyses in PRA as applied to FTA are handled later in the questionnaire)?
   b. Which requirements in it are such that they are better left to other kinds of assessments?
      Why?

3) The relationship between PRA and FTA.
    a. In your view, is PRA useful in FTA? If yes,
        i. what role(s) could PRA play in FTA?
        ii. What are its most useful aspects and uses?
        iii. What supporting analyses would be needed to support PRA for FTA?
    b. If PRA is not useful in FTA, why?
    c. Can FTA benefit PRA?
    If it can, what kinds of FTA analyses or results could be used in PRA?
    Have you used FTA or its results to benefit PRA?

4) Have you used PRA in FTA? You may leave this set of questions unanswered if you answered no to question 1.
    a. If yes,
        i. what role(s) did PRA play in the analysis, and what objectives did it serve (you may refer to your answers to question sets 2 or 3 if needed)?
        ii. What particular SSCs did you address with PRA, and what particular YVL B.1 requirements (if any)? Which (if any) SSCs and requirements did you address with other methods?
        iii. How did you use PRA - what PRA model parts and results did you utilize, did you carry out some PRA analyses specifically for FTA, did you construct some PRA models (event trees, fault trees etc.) specifically for FTA or did you only utilize existing models, did you modify existing PRA models?
        iv. Was PRA useful in these FTA tasks? What FTA analysis tasks you conducted would have been better left to some other method than PRA, and why?
    b. If not,
        i. what are the main reasons for not using PRA?
        ii. What role could PRA play in the analyses you have conducted, if any? Which parts of the plant PRA model could be utilized (whole model, some parts - which ones?)?
        iii. Do you anticipate that some PRA models (fault trees, event trees etc.) would have to be modified or constructed for FTA? What FTA analysis tasks are better left to other methods than PRA, and why?

5) Approach to reliability analysis of digital I&C to support FTA and PRA.
    a. If such an approach were constructed, which YVL B.1 requirements should it address?
    b. What systems (e.g. programmable automation, safety automation, safety systems) should be analyzable with the method?
    c. What kinds of results should it produce?
    d. In what way(s) should the approach support PRA?
    e. In what way(s) should the approach support failure tolerance analyses?
    f. Do you have a problem (system(s), YVL requirement(s), ...) in mind that could be a good case for analysis in NAPRA T4.2?

6) Do you have any comments concerning FTA, or the use of PRA in FTA, that you did not handle in your answers to the previous questions?
Do you have any comments concerning this questionnaire?

7) Information on the respondents

1. Name of the organization

2. Name(s) of the respondent(s) (optional)

Thank you for your answers!